

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

vs.

No. 11 CR 1690 MV

JOHN CROWE,

Defendant.

MEMORANDUM OPINION AND ORDER

THIS MATTER came before the Court on Defendant John Crowe's Motion to Compel (Doc. 53) and Motion for Independent Evaluation by Defense Expert (Doc. 54). The Court has considered the motions, the government's response (Doc. 58), Defendant's reply (Doc. 61), and the relevant legal authority. Being otherwise fully advised of the premises therein, the Court finds the Motion to Compel (Doc. 53) should be DENIED; and the Motion for Independent Evaluation by Defense Expert (Doc. 54) should be GRANTED in part and DENIED in part, for the reasons stated herein.

BACKGROUND

In approximately March of 2011, New Mexico State Police Sergeant Matthew Pilon of the Online Predator Unit searched the CPS database for an IP address in his area that had "previously been identified by other law enforcement as having SHA values related to child pornography." (Doc. 56 at 53.) The CPS ("Child Protection System") database is a law enforcement database that logs dates and times known images of child pornography are made available for sharing from specific IP addresses. Sergeant Pilon received information from CPS that the IP address 69.247.74.20 "had been seen with SHA values that other law enforcement had identified as being child notable." *Id.* at 121. Sergeant Pilon then utilized Shareaza LE to

conduct an investigation into that IP address. *Id.* at 53. Shareaza LE is described as a modified version of the publicly available peer-to-peer (P2P) software, Shareaza. Shareaza LE is modified for law enforcement use to only obtain files from a single IP address, rather than obtaining multiple pieces of a file from multiple IP addresses. *Id.* at 54. Sergeant Pilon testified that Shareaza LE constantly monitors a target IP address waiting for that address “to come up and running.” *Id.* at 56. When an IP address comes up, Shareaza LE attempts to browse files available in the target computer’s shared files. According to Sergeant Pilon, Shareaza LE then searches the browse list of files available for sharing to see if any of the files have values (SHA values) that match the hash values of previously identified child pornography images. *Id.* at 56-57. If there is a match, then the software attempts to download that image from the target computer.

According to the Affidavit for Search Warrant, on March 3, 2011, Sergeant Pilon, utilized the Shareaza LE software and observed IP address 69.247.74.20 offering to share files containing SHA values which had been previously identified as depicting images of child sexual abuse. (Doc. 41-1 at 8.) On this day, Shareaza LE was able to “log and directly download a file from the suspect computer.” *Id.* “[T]he software was also able to download a publicly available listing of a shared file listing from the suspect computer” with “the overwhelming majority of the file names [being] pornographic in nature and many appear[ing] to be directly referencing underage children.” *Id.* According to the Affiant, Agent Joseph Casarez, on March 3, 2011, the target IP address had two images of child pornography with SHA values matching those of known child pornography in its shared files. *Id.* at 8-9.

Sergeant Pilon then conducted an internet search on the origin of the IP address, 69.247.74.20, and found it to be issued to Comcast. *Id.* at 9. Subsequently, Sergeant Pilon

requested the assistance of Department of Homeland Security Special Agent Justin Allen in obtaining a summons requesting the identification of the subscriber using the IP address 69.247.74.20. *Id.*

On April 1, 2011, Comcast identified the subscriber as John Crowe, residing at 6901 Los Volcanes Rd., NW in Albuquerque, New Mexico. A public records check confirmed John Crowe resided at this address. On April 29, 2011, Agent Casarez conducted surveillance at Mr. Crowe's residence and confirmed the location of the residence. Based upon the aforementioned information and the additional information contained in the Affidavit for Search Warrant, Agent Casarez believed he had probable cause to search Defendant's residence for computer and other related items listed on pages 2 and 3 of the Affidavit for Search Warrant. *Id.* at 13.

On May 24, 2011, Second Judicial District Court Judge Pat Murdoch issued a Search Warrant for Defendant's residence based upon the Affidavit for Search Warrant. *Id.* at 1. On May 26, 2011, Agent Casarez, Special Agent Allen and other law enforcement agents with the New Mexico State Police and Homeland Security Investigations (HSI) executed the Search Warrant at Defendant's residence at 6:04 a.m. The officers seized a Compaq Desktop computer and a CD labeled "John & Teresa." *Id.* at 15. While other agents conducted the search of Defendant's residence, Agent Casarez and Special Agent Allen interviewed Defendant. During the interview, Defendant admitted on several occasions he had actively searched for and downloaded child pornography. He also admitted sharing these images with others.

Subsequently, Sergeant Pilon conducted a preview of Defendant's computer and observed child pornography images and videos that appeared to have been taken with a hidden camera. Based upon these findings, on May 28, 2011, an agent contacted Defendant and asked if he would voluntarily speak with the agents at the Albuquerque HSI Office. Defendant agreed

and arrived at the office shortly thereafter where he was advised of his Miranda rights. He then gave a recorded statement acknowledging the images were created with the use of hidden cameras placed in bedrooms and bathrooms of former girlfriends and their minor daughters living in Ohio, Georgia and Alabama. He admitted recording these images for a period of approximately five years and transporting them to New Mexico with him when he moved to Albuquerque. Based upon this additional information and the Application and Affidavit for Search Warrant sworn by Special Agent Allen, a second Search and Seizure Warrant was obtained from U.S. Magistrate Judge Alan C. Torgerson on June 7, 2011 to seize further evidence of the commission of the crimes at issue in this case. (Doc. 41-2.)

MOTION TO COMPEL

Defendant asks this Court to order the government to “disclose all discovery regarding the investigation of Defendant by ‘TLO’ and ‘CPS’ from which the warrant was eventually derived.” (Doc. 53 at 1.) He states he first learned about TLO and CPS at the hearing on his Motion to Suppress, during which he learned that it was information provided by CPS that led to Sergeant Pilon’s investigation of Defendant’s computer activity. *Id.* at 3. Specifically, Defendant is requesting “the names of the employees of TLO and CPS who performed the search, the name and description of all software used, the scope of the search, including the search terms, the areas of the computer searched, the specific results of the search, the name of the suspect files, the location of the suspect files on Defendant’s computer, and the properties of the files found.” *Id.* He requests this information so that his defense expert can independently evaluate the data.

The Court notes that Defendant’s motion fails to cite any legal authority whatsoever in support of his request. However, in his Reply (Doc. 61), he argues TLO and CPS are

government agents whose actions are imputed to the government. *Id.* at 4. He claims the actions of TLO and CPS in this case satisfy the two-part test set forth in *Pleasant v. Lovell*, 974 F.2d 1222 (10th Cir. 1992) for determining when a private party's actions implicate the Fourth Amendment. He argues that to allow "the government to conduct business with these agencies for the purpose of securing search warrants, without any repercussions for violations of the Fourth Amendment, allows for the government to hide behind the actions of unscrutinized agents." (Doc. 61 at 4.) He claims, "[t]his gives the government carte blanche authority to violate the Fourth Amendment through its 'third party entities' with no recourse to the Defendant whose rights have been violated." *Id.*

The government responds to Defendant's argument claiming that TLO and CPS are private entities over which the federal government has no "custody, control or possession" of the information requested as required for disclosure pursuant to Fed. R. Evid. 16(a)(1)(E). The government also argues the requested discovery is irrelevant to a determination of probable cause and immaterial to refuting the government's case-in-chief. *See United States v. Armstrong*, 517 U.S. 456 (1996) (Rule 16 authorizes defendants to examine government documents material to the preparation of the defendant's defense against the government's case-in-chief). Finally, the government argues the discovery sought is shielded from disclosure by the law enforcement privilege.

ANALYSIS

The Court finds Defendant's Motion to Compel vague and largely unsupported. While Defendant cites to three cases in his Reply (Doc. 61) in support of his argument that TLO and CPS are private entities whose conduct should be imputed to the government,¹ he fails to take the

¹ Because Defendant raised the argument that TLO and CPS were private entities acting as government agents for the first time in his Reply (Doc. 61), the government was not given an opportunity to respond to the argument.

next important step of explaining why the information sought is discoverable under Rule 16. Even if TLO and CPS are government agents, Defendant still bears the burden of proving the information sought satisfies the criteria set forth in Rule 16(a)(1)(E).² *See Pleasant*, 974 F.2d at 1226-27 (movant has burden by a preponderance of the evidence to establish the private party acted as a government agent). However, Defendant does not argue or even identify the Rule 16 factors, but instead merely says the information sought is relevant because it goes to the “root of the issue—whether the search of Defendant’s computer, which was the basis of the search warrant, extended into the private sector of his computer, violating his constitutional rights.” (Doc. 61 at 6.) This argument, with nothing more, is speculative and amounts to little more than a fishing expedition into TLO and CPS in hopes of finding something useful. *See United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (“Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.” (citations omitted)).

Disclosure under Rule 16 requires the information sought by Defendant to be in the government’s “possession, custody or control.” Fed. R. Evid. 16(a)(1)(E). Defendant argues TLO is a private agency and CPS is a government agency; both of whom work together to search for child pornography for law enforcement purposes. Consequently, their actions are imputed to the government. Presumably, this argument is intended to support a finding that the information sought is in the government’s possession, custody or control. The government responds that both TLO and CPS are private agencies over which it has no possession, custody or control. Specifically, it states:

² Defendant does not argue the discovery sought requires disclosure pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963) or *Giglio v. United States*, 405 U.S. 150 (1972).

The CPS database was developed for the exclusive use of certified law enforcement officers who specialize in peer-to-peer (P2P) investigations, but it is wholly owned and operated by the private data-fusion company TLO. *See* Attached Affidavit—William Wiltse, TLO. The CPS database aggregates investigative leads generated by law enforcement agencies around the world which utilize different software platforms to identify IP addresses that make known images of child pornography available for download. The software platforms that provide the investigative leads for CPS are based on freely available open source applications that view the “shared” folders of computer users that have voluntarily joined different file sharing networks. *Id.* The software platforms used to populate the CPS database do not have access or query any part of a client computer participating in a file sharing network that has not been made publicly available by the user. *Id.* The federal government does not have custody, control or possession of the databases’ software, source codes or data, nor does it control, direct or supervise any of TLO’s employees. *Id.*

(Doc. 58 at 1, n.1.) In support of its position, the government submits an Affidavit of William S. Wiltse, a former police detective, developer, certified instructor in CPS and the current director of law enforcement programming at TLO. (*See* Doc. 58-1.) Mr. Wiltse states that TLO is a private company in Boca Raton, Florida. *Id.* at 1. He says “CPS focuses on the development of software tools to identify computers trading files depicting the sexual abuse of children and training law enforcement officers in their use.” *Id.* He then describes the manner in which the CPS database is used by trained law enforcement to target IP addresses suspected of possessing and distributing images of child pornography. *See id.* at 2-4.

Additionally, the Court heard the testimony of Sergeant Pilon concerning TLO and CPS. He described TLO as a “private company” owned by an individual in Florida that “provides [law enforcement] with storage, servers and programmers to assist in the investigation of these types of crimes.” (Doc. 56 at 11, 46-47.) “TLO provides the space and the server for [law enforcement] to maintain the [CPS] database.” *Id.* at 46. He then described CPS as “the data set of all this information that law enforcement has collected over the past. . . seven, eight years. As we gather this data, it’s populated up into the CPS system, which is a database. At a bare

minimum, we equate this as the equivalent to a tip from another law enforcement officer. Only law enforcement personnel trained in the ICAC [“Internet Crimes Against Children”] and trained in these investigations is supplying data to the CPS system.” *Id.* at 49.

Based upon the information in Mr. Wiltse’s Affidavit and the testimony of Sergeant Pilon, the Court finds that TLO is a private company not under the government’s control. TLO is owned and operated by a private individual who has donated storage space to house a law enforcement database and who provides programming and training to law enforcement personnel to use in their investigations of child pornography. There is no evidence that TLO or its employees actually conduct the investigations themselves into targeted IP addresses. All of the evidence concerning this matter indicates that the information stored in the CPS system, housed by TLO, is gathered by law enforcement personnel around the world. (*See* Doc. 56 at 49.) Consequently, the Court finds Defendant has failed to meet his burden of showing TLO, a private entity, acted as a government agent. *See Pleasant, supra*. Consequently, the Court finds the information sought from TLO is not within the government’s possession, custody or control; and therefore, does not require production by the government pursuant to Fed. R. Evid. 16(a)(1)(E).

Next, Sergeant Pilon’s testimony and Mr. Wiltse’s Affidavit support a finding that the CPS database is operated and maintained by law enforcement agents. Trained law enforcement personnel access and provide information to the CPS database. The database is used strictly by law enforcement personnel to assist in their investigations of internet crimes depicting child abuse. (*See* Docs. 56 at 49, 58-1 at 1.) Consequently, the Court finds the CPS database is controlled by the government. Therefore, the Court must next determine whether the information sought is material to the preparation of his defense. *See* Fed. R. Evid. 16(a)(1)(E)(i).

In this case, Defendant challenges the extent of the search of his computer, arguing that law enforcement officers may have gone beyond the publicly available files and actually searched private files located on his computer. He seeks discovery to support this theory. If proven, he may have a viable defense to the charges set forth in Counts 3, 5 and 6 of the Superseding Indictment alleging he advertised, distributed and attempted to distribute images of child pornography. If the images found on Defendant's computer were not located in shared space or otherwise made available to the public from Defendant's computer, such a finding would be material to Defendant's defense, and discoverable under Rule 16(a)(1)(E). *See United States v. Armstrong*, 517 U.S. 456, 462 (1996) (Rule 16 permits discovery of documents material to a defendant's preparation of his defense to the government's case-in-chief.).

However, the Court also recognizes that the case-in-chief against Defendant is not based upon the findings of CPS. None of the charges against Defendant in the Superseding Indictment concern information about Defendant's computer found on the CPS database. Counts 3, 5, 6 and 7 of the Superseding Indictment all allegedly occurred on and after Sergeant Pilon's initial investigation into Defendant's computer.³ Therefore, none of the information contained on the CPS database, or the manner in which it was gathered, is relevant to the charges against Defendant. Such information is not material to Defendant's defense against the charges that on or about March 3 and 12, 2011, law enforcement agents observed Defendant offering to share images of child pornography through a P2P website. Even if Defendant could prove that earlier in time CPS had obtained information about Defendant's computer by searching his private files, rather than any made publicly available, such information would have nothing to do with whether or not later, on March 3 and 12, 2011, he offered to share images of child pornography.

³ Counts 1, 2, and 4 are unrelated as well as they concern allegations that Defendant produced child pornography and transported it across state lines.

Consequently, the Court finds Defendant has failed to show the information sought concerning CPS is material to the preparation of his defense against the government's case-in-chief. *See Armstrong*, 517 U.S. at 462; *Mandel*, 914 F.2d at 1219.

MOTION FOR INDEPENDENT EVALUATION BY DEFENSE EXPERT

Defendant asks the Court for an "order permitting defense expert Tami Loehrs to have access to all of the government's software programs used in this case, including the programs used by CPS and TLO, GnuWatch, Peer Spectre, Shareaza LE, and any other software programs utilized, to complete the analysis of Defendant's computer." (Doc. 54 at 1.) He claims the "government used multiple search programs to search Defendant's computer for child pornography." *Id.* at 3. He also states, "the name and nature of the programs are unknown, as is the search procedure used." *Id.* He argues, "[t]he only manner in which Defendant's motion to suppress can be fully litigated, so this court can determine whether the search was constitutional, is to permit Ms. Loehr to perform an independent analysis of the searches conducted using the same software as used by the government. Failure to grant this request yields a one-sided analysis of whether the search was proper as the Defendant cannot challenge the scope of the search without understanding the software." *Id.* He also argues the requested discovery is necessary "to prepare for trial;" and that he has a "right to an independent analysis" of the evidence. *Id.* at 3-4.

The government responds that "Rule 16 does not authorize the disclosure or inspection of proprietary investigative materials, such as Shareaza LE, or the discovery of any underlying data, methods or applications that were used to generate 'the results or reports' described in Fed. R. Crim. P. 16(a)(1)(F)." (Doc. 58 at 12.) The government claims the Tenth Circuit "rejected the type of ancillary discovery request that Defendant now makes", citing *United States v. Price*, 75

F.3d 1440 (10th Cir. 1996). *Id.* It claims to be “unaware of a single federal district court granting the type of access to investigative software applications that Defendant now proposes.” *Id.* at 13. Finally, it claims the information sought is shielded from disclosure by the “law enforcement privilege.” *Id.* at 14-17.

ANALYSIS

The Court finds the requested access “to all of the government’s software programs used in this case, including the programs used by CPS and TLO, GnuWatch, Peer Spectre, Shareaza LE, and any other software programs utilized, to complete the analysis of Defendant’s computer” is overly broad. For the reasons stated previously herein, Defendant is not entitled to access software belonging to TLO and CPS.

However, with respect to the software used by Sergeant Pilon in his investigation of Defendant’s computer, the Court finds instructive the recent Ninth Circuit decision in *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012). In *Budziak*, the Ninth Circuit considered facts very similar to those at issue here. In *Budziak*, the FBI used EP2P to investigate the defendant’s computer. EP2P is described as a modified version of LimeWire, a publicly available P2P file-sharing program that allows users to search for and download files stored on other users’ computers. Like Shareaza LE in this case, EP2P “purportedly allows the FBI to view all files that a particular user on the file-sharing network is making available for download by other users at a given time.” However, as in this case, the FBI software, EP2P is enhanced to download complete files from a single user, rather than downloading pieces of files from multiple users. This allows law enforcement to target one individual IP address to determine if that address has a complete copy of the suspect file. The use of the EP2P software led to a search warrant for Budziak’s computer.

During discovery, *Budziak* moved to compel discovery of the EP2P software. Like here, Budziak specifically requested disclosure of the EP2P program and its technical specifications. He argued that evidence suggested “the FBI may have only downloaded fragments of child pornography files from his ‘incomplete’ folder, making it ‘more likely’ that he did not knowingly distribute any complete child pornography files.” 697 F.3d at 1112 (citation omitted). Budziak also “submitted evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings.” *Id.* Nevertheless, the district court denied Budziak’s motions to compel discovery concerning the EP2P program.

On appeal, the Ninth Circuit noted that “[a]lthough Budziak had an opportunity to cross-examine the government’s EP2P expert, he was denied background material on the software that could have enabled him to pursue a more effective examination.” *Id.* The Ninth Circuit cited with approval the Third Circuit, which held: “A party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately.” *Id.* (citing *United States v. Liebert*, 519 F.2d 542, 547-48 (3d Cir. 1975) and *United States v. Di-oguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970) (“It is quite incomprehensible that the prosecution should tender a witness to state the results of a computer’s operations without having the program available for defense scrutiny and use on cross-examination if desired.”)). The Ninth Circuit concluded the district court abused its discretion by denying Budziak discovery on the EP2P program, stating as follows:

Although the government argued that the computer logs it provided Budziak demonstrated that he would not uncover any helpful information through discovery of the software, the declarations of Budziak’s computer forensics expert stated otherwise. In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless. While we have no reason to doubt the government’s good

faith in such matters, criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary. This is especially so where, as here, a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software.

Id. at 1112-13 (notation omitted).

This Court finds the Ninth Circuit's analysis in *Budziak* persuasive and notes that the Tenth Circuit has not yet addressed a similar issue. As in *Budziak*, in this case, Defendant submitted the testimony of his expert witness, Tami Loehrs, who indicated that during her examination of Defendant's computer, some of the files alleged to have been found by law enforcement in the shared space of Defendant's computer, were not found there during her analysis. Defendant is entitled to test the reliability of the computer evidence used against him, especially because it is the basis of the government's case-in-chief.

Furthermore, the Court does not agree with the government's argument that the evidence sought is "ancillary" as discussed in *United States v. Price*, 75 F.3d 1440 (10th Cir. 1996). The evidence sought in this case is quite critical to the government's case-in-chief against Defendant. Defendant is not obligated to merely defer to the government's word that his own separate investigation would be unfruitful. *See Budziak*, 697 at 1113. Additionally, the facts in *Price* are distinct from those at issue here. *Price* is a drug case in which the defendant sought discovery of: 1) the underlying basis of a chemist's conclusions that the substance tested was methamphetamine; 2) information relating to the reliability of the chemist's equipment; and 3) evidence of the chemist's credentials. 75 F.3d at 1444. The Tenth Circuit concluded that Rule 16 only obligated the government to turn over the report and results of the chemist's analysis, and not this additional evidence concerning the chemist's process and background. However, the same rationale does not apply to a computer investigation in which the only software at issue

is within the government's sole possession. *See Liebert, supra; Di-oguardi, supra*. Unlike drug cases, in which a defendant can obtain his own equally qualified chemist to conduct an assessment of the substance at issue, a defendant cannot simply replicate a search of his computer using different software not modified with the same specifications used by law enforcement. Consequently, the Court does not find the government's argument persuasive.

Finally, the Court also rejects the government's argument that the law enforcement software used to investigate Defendant's computer is protected by the "law enforcement privilege." (*See* Doc. 58 at 14-17.) The government argues the privilege is designed "to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." (Doc. 58 at 15 (citing *In re Dep't of Investigation of City of New York v. Myerson*, 856 F.2d 481, 484 (2d Cir. 1988)). However, the government fails to show how the software used by Sergeant Pilon to search Defendant's computer falls within this exception. The government does not argue that any confidential sources, witnesses or law enforcement personnel are at risk or that their privacy may be compromised by the disclosure of the software. Nor does it argue interference with an ongoing investigation. Only the potential disclosure of law enforcement techniques and procedures appears to be at issue. However, while the government persists the software is proprietary, it is not secret. Sergeant Pilon testified at length about the software, its specifications and the manner in which it is modified and used. Other than broadly asserting privilege and harm, the government has not identified any actual harm that may arise from allowing Defendant's computer expert access to the software for purposes of running a controlled test on Defendant's computer. The Court itself can see no harm in allowing

the testing. Consequently, the Court finds, pursuant to Rule 16(a)(1)(E), the government is required to produce to Defendant the software, Shareaza LE, and any other software used by Sergeant Pilon to conduct his initial investigation of Defendant's computer. The government is also required to produce to Defendant any software used by law enforcement to analyze Defendant's computer after Sergeant Pilon's initial search, the results of which it intends to use during its case-in-chief at trial. Any software sought by Defendant not used in this case is not discoverable.⁴ Furthermore, the software will be subject to a protective order as described below.

IT IS THEREFORE ORDERED that Defendant's Motion to Compel (Doc. 53) is hereby DENIED.

IT IS FURTHER ORDERED that Defendant's Motion for Independent Evaluation by Defense Expert (Doc. 54) shall be DENIED as to TLO and CPS; and shall be GRANTED with respect to the software Shareaza LE and any other software used by Sergeant Pilon or other law enforcement officers in their investigation of Defendant's computer in this case.

IT IS FURTHER ORDERED that the law enforcement software Shareaza LE and any other software required to be produced by the government pursuant to this Order shall be subject to a protective order. The protective order shall be prepared and submitted to the Court by the government, with defense counsel approval, no later than seven (7) days after entry of this Order. The protective order shall require the defense expert to examine the software at issue at a designated law enforcement facility, at a mutually convenient date and time, for as much time as


⁴ Defendant requests disclosure of the following software: GnuWatch, Peer Spectre, Shareaza LE, and any other software programs utilized. Sergeant Pilon testified that he used Shareaza LE to search Defendant's computer. Therefore, Shareaza LE shall be made available to the defense expert. The Court is not aware of any other software used in this case. However, to the extent that law enforcement did use additional software in its investigation of Defendant's computer, that software shall be identified and also made available to Defendant's computer forensics expert.

is reasonably necessary for the expert to complete her examination. No copies of the software shall be made. The software shall not leave the custody of the law enforcement agency that controls it. Any proprietary information regarding the software that is disclosed to the defense expert shall not be reproduced, repeated or disseminated in any manner. Violation of the protective order shall subject the defense expert and/or defense counsel to potential sanctions by this Court.

IT IS FURTHER ORDERED that the examination of the software at issue shall be completed no later than forty-five (45) days from entry of this Order. Thereafter, Defendant shall have fourteen (14) days to file a supplemental brief to his Motion to Suppress (Doc. 36). The government shall have fourteen (14) days to file a response. Defendant shall then have seven (7) days to file a reply. If either party believes additional testimony is necessary concerning the Motion to Suppress based upon the additional discovery and briefing, then that party shall notify the Court of the need for an additional hearing on the motion in its filing with the Court.

IT IS FURTHER ORDERED that this Court's decision on the Motion to Suppress (Doc. 36) shall be STAYED until discovery and additional briefing is completed in accordance with this Order.

DATED: April 3, 2013.



MARTHA VÁZQUEZ
U.S. DISTRICT JUDGE